AIR WAR COLLEGE

AIR UNIVERSITY

# TARGETING JOHNNY:

# ANALYZING THE LEGALITY, LEGITIMACY, & POLICY IMPLICATIONS OF AN ENEMY ATTACK ON CONUS RPA UNITS



by

James L. Chittenden, Lieutenant Colonel, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Kimberly A. Hudson

14 February 2013

## DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

# Biography

Lieutenant Colonel Jim Chittenden is a United States Air Force officer assigned to the Air War College, Air University, Maxwell AFB, AL. He graduated from Duke University with a Bachelor of Science degree in Mechanical Engineering, the University of Arkansas with a Master of Science degree, and the Air Command and Staff College with a Master of Arts degree. He earned his pilot wings in April 1998 at Sheppard AFB, has over 3,500 flying hours in the MQ-9, B-1, and F-15C/E, and is a graduate of the United States Air Force Weapons School. Colonel Chittenden is a fully qualified Joint Officer, a member of the Acquisition Corps, and a graduated squadron commander.

# Abstract

The United States military's use of remotely piloted aircraft (RPA) has skyrocketed since 2001. Many military analysts believe this trend will continue, with unmanned systems representing the future of aerial warfare. In fact, in the near future, RPA operations may not exclusively be a virtual "away game." While RPA employment to date has focused on non-state actors and terrorists, operations against other sovereign states render the US RPA infrastructure a legal and legitimate target. This paper's thesis addresses this fact and the related implications of placing personnel, property, and civilians near RPA garrisons at risk.

The paper first describes the key operational elements of the RPA enterprise, demonstrating it is a "system of systems" including air, space, and cyber operations spanning the continental US (CONUS) and other countries. The paper then introduces an analytical framework for determining the legality and legitimacy of target sets using the Articles of the Geneva Convention, US and international case law, and just war theory. Through this analysis, it demonstrates that the preponderance of the CONUS RPA infrastructure is both a legal and legitimate target for sovereign states engaged in conflict with America. The paper then documents that neither Department of Defense nor service policy has addressed this vulnerability by providing specific examples of the alarming degree to which US combat capability would be degraded by adversary attacks on RPA operations in the homeland. It then presents several detailed prescriptions for consideration and action. Finally, the paper concludes with a discussion of some related implications of geographically dislocated warfare.

# Fictional Vignette & Introduction

(The future) On July 12, 2015, conflict with Venezuela boiled over into America. In the preceding two years, US Southern Command's newly allocated fleet of MQ-9 Remotely Piloted Aircraft (RPA) discovered evidence the Venezuelan government was housing and funding training camps for militant groups connected with Al Qaeda. Following repeated diplomatic warnings, the US intensified activities from Phase 0 Shaping Operations to limited deterrence actions and overflight of sovereign Venezuelan soil. In early 2015, the Intelligence Community linked violent protests at the US embassy in Caracas, including rocket attacks into the compound, to Venezuela-backed terrorist organizations. In response, the US struck the militant training sites utilizing JDAM-equipped MQ-9s, and an open state of hostilities ensued.

Over the next several months, Venezuelan Special Operations Forces (SOF) planned offensive operations to end the Air Force's use of RPAs, hoping to diminish a clear asymmetric advantage of the US. This culminated in coordinated physical and cyber-attacks against the RPA enterprise in and around Syracuse, NY. First, SOF teams targeted the Syracuse electrical grid cutting off power to both the Air Force Base and a city of 140,000 people. Then they struck the base itself destroying aircraft hangers, buildings, satellite dishes, and the Communications Squadron. This devastated the base's network capability and resulted in massive casualties of civilian, contractor, and military personnel completely overwhelming the local hospital's capacity. Prior surveillance also identified base leadership personnel -- the Wing Commander was targeted at Wing headquarters, while the Command Chief was attacked during his transit to base. SOF teams attacked key personnel from two squadrons, including an active duty and National Guard squadron commander, destroying their residences and their next-door neighbors'.

An enormous civil-military leadership crisis ensued as the surrounding area's economy

was wrecked, and the local populace was enraged at both Venezuela's audacity and the US military's unpreparedness. A larger debate occurred in Washington DC on Venezuela's actions as the US government attempted to divert scrutiny of its policies and readiness by portraying the attacks as acts of terrorism. At the United Nations, Venezuela responded that the attacks were legitimate and legal acts of self-defense in light of US attacks in Venezuela. Weary of the US's universally unpopular use of RPAs, the majority of the world's nations agreed with Venezuela, and America did not fly another drone in the conflict.

(2013) The US military's use of remotely piloted aircraft has skyrocketed since September 11th 2001. Further, owing to a decade of success in the Global War on Terror and optimized for an increasingly resource-constraint budget environment, RPA operations will almost certainly intensify in the future, even if the US's present technological monopoly is short-lived.[a] In fact, many military analysts predict unmanned systems will be the future of aerial warfare, largely, if not completely, supplanting manned aircraft in several mission areas.[1]

While past RPA operations have focused on non-state actors and terrorists, RPA employment against other sovereign states potentially renders the United States' RPA infrastructure a legal and legitimate target. This may undermine one of the benefits of unmanned systems, as RPAs are ideally suited for reducing risk to aircrew in their theater of operations. Indeed, future security scenarios employing RPAs may place personnel, property, and civilians near their garrisons at realistic risk of legitimate attack. The Department of Defense (DOD) must explore this topic and address associated vulnerabilities with specifically formulated policy solutions.

This paper first describes key operational elements of the RPA infrastructure. It then

[a] According to the DOD's Unmanned Systems Roadmap 2011-36, $32B is planned on unmanned systems between 2011-15. In addition, 40 countries are working on military robotic platforms.

introduces an analytical framework for determining the legality and legitimacy of targets. It applies a taxonomy demonstrating the preponderance of the continental US (CONUS) RPA infrastructure is both a legal and legitimate target for sovereign nations engaged in conflict with America. The paper then details that neither DOD nor service policy has addressed this vulnerability and presents several prescriptions for consideration and action. Finally, the paper concludes with a discussion of the future implications of geographically dislocated warfare.

## RPA Infrastructure & Architecture

MQ-1 Predator and MQ-9 Reaper RPA are integrated systems of systems enabling command and control of airborne elements over distances of thousands of miles. Most USAF RPA are operated beyond-line-of-sight by mission control elements at CONUS locations in an employment concept called Remote Split Operations (RSO). RSO highlights a capability inherent to RPAs to produce sustained combat capability with reduced forward footprints while providing the ability to flex assets between areas of responsibility based on national priorities. The crew and aircraft can re-role to any component of a kill chain during one mission while performing a variety of other mission tasks.[2] Figure 1 represents a notional RSO architecture:

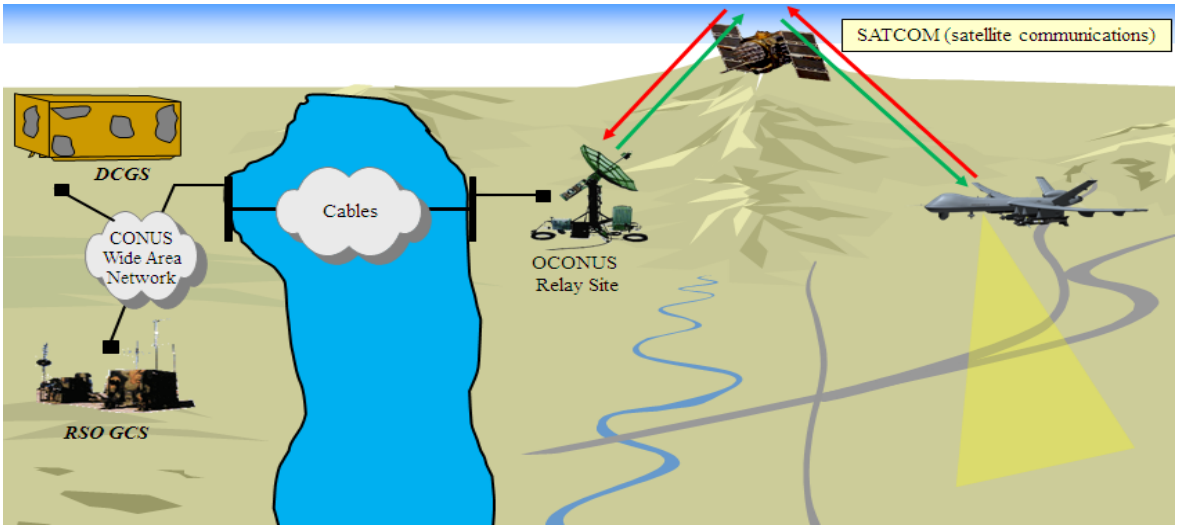


***Figure 1. Architecture of Remote Split Operations***

In this scenario, aircrew in a CONUS Ground Control Station (GCS) fly overseas aircraft via RSO with intelligence support from a CONUS-based Distributed Common Ground System (DCGS). Flight control and sensor inputs are transmitted via fiber optics from the GCS through wide area networks and communication relay sites/nodes to an OCONUS satellite relay site that transmits and receives signals via satellite communications to aircraft in theater. This technology chain extends from the US to above other nations and contains numerous civil, military, dual-use, and international components of varying degrees of vulnerability and susceptibility to legal and legitimate attack.

## Analyzing Legality & Legitimacy

Laws governing armed conflict and just war theory provisions extend to all the locations of all participants in a conflict. In fact, international law has never recognized geo-political boundaries as limiting a nation's freedom to act in accordance with the provisions of the Hague or Geneva Conventions.[3] Article 52 of the Additional Protocol to the Geneva Conventions simply states attacks should be limited to military objectives, "objects which…make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[b] The interpretation of "military objective" is significant when discussing dual-use infrastructure -- objects including power sources and grids, transportation networks, and telecommunication systems serving both military and civilian purposes.[4] Such targets are examined for proportionality -- whether targeting them would cause excessive damage in relation to any achievable direct or concrete military advantage.[5] Importantly, the DOD has held "objects used concurrently for civilian and military purposes are liable to attack if there is a military advantage to be gained in their attack."[6]

[b] Although the US is not a signatory to the Additional Protocol, according to AFDD 3-60, *Targeting*, it views this definition as an accurate restatement of customary international law.

The US should assume a similar liberal legal interpretation by its enemies and expect the same rules to apply to any adversary attack against the homeland.

The legal definition of a combatant is equally significant as it affords the "right to participate directly in hostilities." According to the Geneva Convention, members of any armed forces of a party in a conflict are combatants. This consists of all organized armed forces, groups, and any organized units under a command responsible for its subordinates' conduct.[7] Further, the US Military Commissions Act of 2006 defined lawful combatants as uniformed "members of regular forces…belonging to a state engaged in hostilities…"[8] However, in combatant status, there exists a duality. While it grants combatant privilege, it also subjects an individual to attack at any time by other parties to the conflict. A combatant may be "lawfully targeted whether or not they are posing a current threat to opponents and whether or not they are armed."[9] Regarding the basic legal principles of armed conflict, the USAF has simply stated, "Military facilities and forces…are targets anywhere and anytime."[10]

From a legal perspective, the RPA enterprise exemplifies a steady and continuous shift of hostilities into population areas. This has led to increased intermingling of civilians with both combatants and military targets, and has facilitated their involvement in activities historically reserved for military operations.[11] Post-9/11, the increased outsourcing of traditionally military functions has inserted private contractors, civilian aircrew and intelligence personnel, and other civilian government employees into the realm of modern armed conflict. This has occurred for both resource and freedom of action considerations. As a result, as operations continue to become more complex involving the coordination of a greater variety of interdependent human and technical resources from different locations, the status of non-uniformed civilian participants in warfare becomes even more significant.[12]

Civilians are afforded protection from targeting "unless and for such time they take direct part in hostilities."[13] The defined determinative act of direct participation is engaging in attacks or in military operations "preparatory to an attack." There is no distinction between government civilians and civilian contractors as it relates to these actions -- neither becomes combatants and both lose protected status. Further, according to the Red Cross, this loss of legally protected status extends for the entire duration of the direct participation and during preparatory measures preceding action, including deployment to and return from the location of action.[14] Still, as practitioners of the profession of arms, DOD personnel should be equally concerned with targeting legitimacy as well as targeting legality, and appropriately distinguish between the two.

While the established laws of armed conflict, derived from customary international law and treaties, govern the legality of targets, the legitimacy of targeting is informed by just war theory, specifically *jus in bello* deliberations. A legitimate targeting decision must first meet legal targeting thresholds and then must be consistent with *jus in bello* (law in war). The three *jus in bello* provisions apply to all parties in a conflict regardless of the reasons for the conflict and whether the cause for conflict is just.[15] First, according to the principle of discrimination, non-combatants must not be deliberately, intentionally attacked. Further, a legitimate act must "not violate the rights of the people against whom it is specifically directed." Here, by virtue of their status, combatants and those taking part in deliberate hostile acts surrender their rights to protection from attack.[16] Second, according to the principle of proportionality, military targets may only be attacked when their military value outweighs the foreseeable destruction that could result. Planners and commanders must weigh the expected military advantages anticipated from kinetically or non-kinetically servicing a target against the incidental loss or injury to civilians and the damage of civilian property.[17] Third, combatants must not use prohibited or illegal

weapons, such as choking agents.[18]

The doctrine of double effect underpins *jus in bello* theory. First proffered by Saint Thomas Aquinas, it postulates it is permissible to perform an act likely to have negative consequences, if four conditions are met:[19]

1. The act or desired end is good in itself (it is a legitimate act of war);
2. The direct effect is morally acceptable;
3. Only a good effect is intended as the principal outcome of the act; and
4. The good effect must proportionally outweigh the negative effect.[20]

Historically, with the US homeland separated geographically from combat zones, uniformed and civilian leadership's double effect determinations have focused on collateral damage, effects, and consequences in far-away foreign lands. However, a RPA aircrew's undeniable combatant status brings the battlefield back home, with serious implications for proportional risk calculations of resident personnel, civilians, and infrastructure. (This is particularly true with dual-use entities, as it is likely very difficult for adversaries to discriminate, and thus destroy only the military portion of dual-use facilities.) This is a significant concern, and the following section demonstrates the alarming degree to which the RPA enterprise is liable to legal and legitimate attacks.

## Applicability to the RPA Enterprise

Article 51 of the United Nations Charter provides the right to self-defense if armed attacks occur against a member nation.[21] Self-defense not only satisfies the just cause principle of *jus ad bellum* (right to war), but is also the legal authority the US cites for its targeted strikes against Al Qaeda operatives.[22] The US has also asserted an inherent right to self-defense allowing it to target those individuals or groups engaging in or planning attacks against

America.[23] Correspondingly, however, once armed conflict commences, any sovereign UN member is comparably justified in striking the US and all major elements of the RPA enterprise in the homeland.

Fundamentally, in that light, all existing RPA systems on military installations are legal and legitimate targets. This includes aircraft, ground control stations, satellite dishes, lines of communications, computer networks and nodes, supply facilities, operations buildings, and headquarters.[24] Other base facilities such as dining halls, postal offices, and gyms, further away from the RPA chain of operations are also legal targets, but from a legitimacy standpoint require greater scrutiny to establish the proportional military advantage that would ultimately legitimize strikes against them. This, of course, assumes an adversary has adequate pre-strike surveillance to discriminate the main purpose of one facility from another on base.

Similarly, a DCGS providing intelligence support, geographically separated from both the RSO location and the area of responsibility, is liable to attack. This is wholly problematic to the Intelligence Community because each DCGS has the capability to swap its support actions almost hourly between theaters of operation. One day it may be providing processing, exploitation, and dissemination support for combat operations against a nation-state and the next day it may be supporting basic qualification training in the CONUS -- a significant difference in its targetable combat posture. Again, this distributed and shifting mission puts an unrealistic onus on attackers to discriminate when a DCGS is in full combat mode and when it is not.

Further, with the RPA support system stretching over several states and, in some cases, several countries (due to fiber optic lines of communication, network nodes, overseas DCGSs, and satellite farms), exposure to legal and legitimate attack extends well beyond the local municipalities surrounding their RPA bases. This reality could be alarming to a foreign ally or

coalition partner whose civilians are unknowingly and unwittingly put at risk due to collateral damage. This risk would certainly affect the degree to which a country hosting part of the RPA infrastructure has a "red card" veto over US military operations. Accordingly, this veto could be fractious and destabilizing to the very coalitions that enhanced the multi-lateral *jus ad bellum* legitimacy of the military action in the first place.

Attacks against personnel in the RPA enterprise are divided into two distinct categories, military and civilian. All military personnel (except those in protected status such as chaplains, medics, wounded, surrendering, or aircrew parachuting from disabled aircraft) are legal targets whether on-duty or off-duty, on-base or off-base, and in uniform or out of uniform. Similarly, Reservists and National Guardsmen, who presently make up a significant portion of the RPA crew force, are legal targets when activated into either Title 10 or Title 32 status. They lose their civilian protection until the "member disengages from active duty and re-integrates into civilian life, whether due to a full discharge from duty or as a deactivated reservist."[25] Thus, the legitimacy of targeting RPA military personnel off-base or while in transit to base would not be subject to legal review, rather only a determination of discrimination and proportionality. Further, targeting particular leaders of the RPA enterprise in the CONUS is entirely lawful under international law and a just act in the just war tradition.[c] This is because targeting specific military leaders serves to narrow the focus of force employment thus potentially avoiding "broader harm to civilians and civilian objects."[26]

All government civilian personnel and contractors at RPA bases are legal and legitimate targets when directly participating in hostilities. The Red Cross's internationally recognized

[c] While some argue using lethal force against specific individuals fails to provide adequate process and constitutes unlawful extrajudicial killing, this is not the US's view. In 2010, the US State Department's legal advisor stated, "a state engaged in armed conflict…is not required to provide targets with legal process before it uses lethal force."

standard for direct participation is direct causation, an act constituting an integral part of a concrete and coordinated tactical operation causing harm.[27] This includes the loading of mission specific fuel, stores, and data into any part of a RPA system employing lethal force, as well as flying and repairing RPA systems. Likewise, if carried out before the execution of a specific hostile activity such as a RPA combat mission, all of the following constitute preparatory measures and are defined as direct participation in hostilities: equipping, instructing, and transporting personnel; gathering and processing intelligence; and preparing, transporting, and positioning weapons and equipment.[28]

Further, civilians deploying to and from the location of their direct participation lose protection until accomplishing an affirmative act of disengagement, such as arriving at their homes. This means a GCS maintenance contractor is targetable, subject to an adversary's ability to discriminate one civilian from one another, to and from base until he reaches his house. Conversely, civilians maintaining base landscaping or working in dining halls lack causal links to hostilities and therefore are not legitimately targetable. Still, their activities or location may expose them to increased risk of incidental death or injury even if they do not take a direct part in hostilities.[29]

Finally, the General Atomics (GA) factory complex in California, containing both the production plant and the logistics depot for the MQ-1 and MQ-9, presents an area for concern. Consistent with Article 52 of the Geneva Convention, the plant and depot facilities, as with nearly every armament factory making direct contributions to a military campaign, are legal and legitimate targets. In addition, destroying the military's capability to produce and sustain RPAs would undoubtedly pass almost any military planner or legal reviewer's proportionality test. However, according to the Red Cross, while uniformed military personnel at GA are targetable

combatants, civilian workers are merely indirect participants "building up the capacity of a country to harm its adversary," but not directly causing harm themselves. Thus, factory workers as a class should not be subject to specific enemy targeting.[30] In addition, targeting individual civilian personnel at the plant (such as the chief research scientist or lead supervisor) does not meet the threshold of military necessity that could legitimize attacks against them.[31] Consequently, harm to civilians should only be the indirect result of proportionally acceptable attacks on the physical facility itself. Still, GA's facility presents an incredibly attractive singular target to any adversary attempting to destroy America's RPA capability.

## Current Policies

One may contend it is unlikely an adversary would strike the United States' RPA infrastructure because of concerns about provoking a post-Pearl Harbor or post-9/11 response. Certainly, from a military perspective, an adversary would weigh the potential costs of such an attack against the possible advantages of reducing a key US asymmetric technological advantage. It is similarly evident the widespread disapproval of RPAs by other countries (shown in Figure 2) could bolster foreign internal support for strikes against the US and its "technological hegemony."[32] This domestic confirmation would at least influence and perhaps change an adversary's decision calculus by lowering the threshold for direct military action against the RPA enterprise. As such, having demonstrated a strike on CONUS RPAs is both legal and legitimate in the evolving environment of dislocated warfare, one must examine current US policies with the anticipation of a future attack.

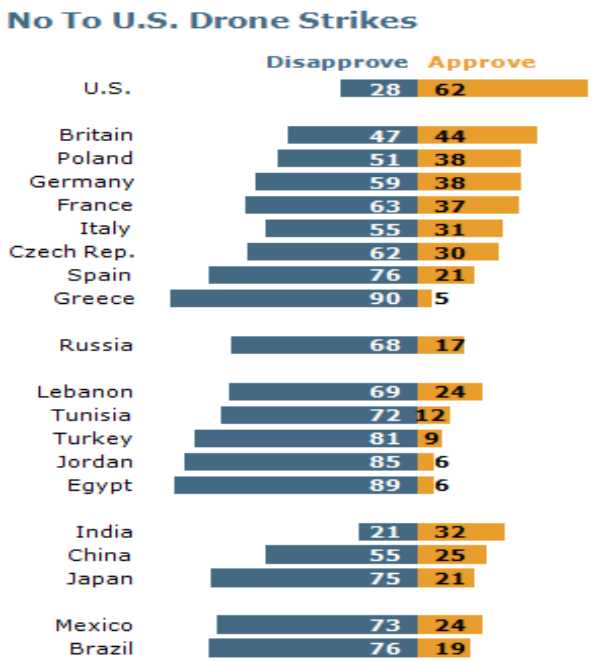


***Figure 2. International Public Support for RPAs, 2012***[33]

In short, policy in this area is extremely limited. Today, the USAF is focusing on building counter-RPA strategies as well as developing technologies, policies, and procedures to defend American capabilities almost exclusively in theater. Lt Gen Larry James, AF/A2, stated, "We recognize that RPAs are important to foreign nations…It's an area where we want to use our capabilities [as well as] deny adversaries the ability to use their RPAs."[34] This is instructive as it belies a blind spot in the military's current thinking -- if the US is examining ways of denying adversaries, then adversaries are most assuredly examining various ways to diminish US capability, particularly in the homeland. In the last four years, all four Services as well as the Department of Defense have published documents detailing their visions and goals for unmanned

combat.[d] None of these documents, however, addresses the vulnerability and susceptibility of the CONUS RPA infrastructure to legitimate and legal attacks by foreign nations.[35]

Further, current law of armed conflict (LOAC) training and instructions for RPA aircrew concentrate solely on tactical employment considerations and theater rules of engagement. While these are undeniably topmost considerations, there is no discussion in required LOAC training on the legality and legitimacy of enemies striking US personnel in the homeland despite specially designed and mandated LOAC modules for RPA aircrew. Further, during combat operations in Libya in 2011, the most prominent example of RPA employment against another sovereign nation-state, the military did not address the fact that its targetable status had changed. Consequently, as doctrine, training, and practice have not addressed this topic, the next section focuses on specific prescriptions for policy-maker consideration.

## Recommendations

First, the military must address the RPA enterprise's susceptibility to legal attacks in its various department and service strategies. According to AFI 36-3204 (Air Force Operations & the Law), it is a commander's obligation to "minimize collateral injury to the civilian population not directly involved in the war effort."[36] While continued RPA combat operations from the CONUS do not rise to the prohibited level of using "civilian populations to shield military forces," it certainly puts the civilian populace and infrastructure around RPA bases in

[d] The USAF released its "Unmanned Aircraft Systems Flight Plan" in 2009 outlining an actionable plan across the spectrum of doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy. In 2009, the US Army published the "Unmanned Ground Systems Roadmap" providing a common basis for Army and Marine Corps (USMC) stakeholders in unmanned ground vehicles (UGVs). The Army released its unmanned aircraft systems (UAS) Roadmap in 2010, establishing a broad vision for developing, organizing, and employing UAS across the spectrum of Army operations. In November 2009, the USMC published its "Concept of Operations for USMC Unmanned Aircraft Systems Family of Systems." Finally, the US Navy published its "Information Dominance Roadmap for Unmanned Systems" in December 2010.

measurably increased peril.[37] This is a moral issue as well as an operational issue. Commanders must anticipate this vulnerability, as the enemy's intent to exact harm or not does not obviate the military's responsibility to see, address, and plan for it. Overall, military and civilian leadership in the Air Force must re-think the nation's proportionality analysis on RPAs, specifically taking into consideration the unintended civilian and military destruction and casualties in the homeland that could result from RPA operations overseas. Then Congress and the military must appropriately resource all identified risk mitigation measures.

To aid in this analysis, the USAF should utilize red teaming. The Joint Staff/J-7 has red teaming expertise to help study and identify vulnerabilities, and then define resourcing solutions and recommendations across the DOTMPLF.[e] It also needs to define classified and unclassified enhancements to the USAF's tactical deception program specifically tailored to the growing RPA enterprise. The magnitude of the RPA community, now at 13 locations in the CONUS and growing, is far beyond the initial concept for the weapon system and its basing distribution. Simply put, the enterprise has expanded so quickly to support the Secretary of Defense's mandate for 65 RPA Combat Air Patrols, this enemy targeting issue may be an example of the axiom, "you can't see the forest for the trees." Still, one vital output of red teaming is to identify which dual-use facilities are most at risk and why. The military must then communicate this potential risk to local civilian leaders and take measures to reduce potential impacts to the civilian populace, including funding parallel military systems where appropriate.

This examination will have some pointed budget implications. First, the USAF needs to adjust its LOAC training for both RPA aircrew and the legal community to add sections on LOAC considerations for CONUS personnel. This should be part of the curriculum at all Major

[e] DOTMPLF - Doctrine, organization, training, materiel, personnel, leadership, and facilities

Command Squadron Commander training courses as well as at the USAF's Wing and Group Commander training. Further, support organizations at RPA bases should receive this training ensuring all military personnel, including bus drivers, telephone operators, etc., fully understand they are legally targetable combatants. Finally, the USAF must recognize the potential for combat losses and program replacement assets for all major elements of the RPA operations chain in the same manner it budgets for and maintains backup aircraft inventory (BAI). This includes, at a minimum: aircraft, GCSs, satellite dishes, computer servers, ground data terminals, and network switches and fiber.

***Figure 3. Mobile Ground Control Station (GCS)***

The USAF needs to acquire and utilize mobile GCSs (figure 3) versus "fixed-facility" GCSs.[f] This tactical level solution has potentially positive strategic effects, as GCSs are clearly lucrative targets for any adversary hoping to neutralize RPA operational capability. Mobile GCSs provide the ability to disperse threatened assets and limit the collateral damage that would occur to any buildings housing fix-facility GCSs. This procurement strategy, combined with requiring Protection Level (PL) 2 security around critical RPA infrastructure elements at all RPA bases, will enhance the community's security posture. (PL2 applies to major components of

[f] Fixed-facility GCSs are housed in specially-configured rooms in permanent structures.

weapons systems that are not on alert status, but are on bases and sites from which they could launch direct strikes against the enemy.)[38] This is especially relevant at Air National Guard (ANG) bases co-located with civilian airfields, as it is imperative the active-duty USAF and the ANG unmistakably communicate risk to local civilian leadership.

Accordingly, the USAF must expand exercise and disaster response plans at all RPA bases to include combat response scenarios. This must go beyond simply augmenting current Active Shooter scenarios. These must be integrated civilian and military engagement opportunities dealing with complex questions arising from combined responses to combat operations, injuries, and damage in the CONUS. It is most appropriate these exercises occur under the umbrella of the National Incident Management System (NIMS), a Department of Homeland Security program. NIMS provides a consistent nationwide structure and approach to enable the government at all levels (federal, state, tribal, and local), the private sector, and select nongovernmental organizations to work together to prepare for, prevent, respond to, recover from, and mitigate the effects of incidents regardless of the incident's cause, size, location or complexity. NIMS delivers a key framework for efficient and effective responses, ranging from a single agency fire response to a multiagency, multijurisdictional natural disaster or terrorism response.[39] It is wholly appropriate base and dual-use facility attack scenarios be first table-topped and then exercised at all municipalities surrounding RPA bases. This is particularly critical for National Guard RPA units as there are numerous additional Title 32 and Title 10 non-combatant status response considerations for guardsmen and their communities.

Finally, the Air Force should consider targeting susceptibility, both from legitimate adversaries and from terrorists, in its decision calculus for future RPA bases. This could increase consideration of more remote bases for future RPA mission expansion. Such a calculus could be

potentially problematic for the ANG as the flourishing MQ-1 and MQ-9 enterprise preserves mission and personnel at bases losing manned aircraft. These bases are typically near populous cities including, in several instances, state capitals. Further, RPA bases should consider housing key leadership personnel in a mix of both on and off-base locations. Similar to not parking combat aircraft close to each other when sabotage is suspected, this strategy could provide a measure of protective dispersion. Overall, the US military must progressively acknowledge that RPA bases are prime targets for all adversaries.

## Future Implications

As the US military increasingly pursues geographically dislocated warfare, similar homeland defense considerations exist to those addressed in this RPA-focused paper. Three specific areas of emerging focus, Cyber Operations, Space Operations, and Global Strike, share a concept of operations from the CONUS. In cyber operations, the US military is still defining what the mission area means. To point, new USAF Chief of Staff General Mark Welsh III stated, “I'm just not sure we know exactly what we're doing in it yet, and until we do, I'm concerned that it's a black hole."[40] Still, cyber networks are notable dual-use systems with both offensive and defensive capabilities. Legal experts have proffered that once cyber-activity equates to the kinetics of a traditional armed attack, the law of armed conflict applies.[41] Further, this technological expansion of the battlefield commands that competent legal advisors on national security matters become substantive learners on all emerging instruments of combat.[42]

Similarly, the USAF is investing in its Global Strike capability, including the embryonic development of a Next Generation Bomber. The ability of the military to hold targets at risk from strategic distances, principally through bomber aircraft and Intercontinental Ballistic Missiles (ICBM) launched from the CONUS, will further emphasize combat operations initiated

from the homeland. In this regard, Air Combat Command and Global Strike Command bomber and ICBM bases should examine their strategic susceptibility to legitimate adversary targeting. USAF Space Command must also accomplish this analysis at its bases as any future conflict with near-peer enemies could well "spill out of the atmosphere" and become a war of satellites.[43] This would carry an additional group of USAF bases into a legal and legitimate targetable status.

Complicating this is the National Guard's growing appetite for other mission sets. Lt Gen Harry Wyatt, former director of the Air National Guard, stated, "'We already know we are going to have fewer airplanes in the future' as he urged Air Guard members to embrace other missions, RPAs and cyber technologies in particular. 'Looking ahead, these are emerging technologies and concepts that could grow even in times of declining economy.'"[44] To what degree does a future threat alter the ANG's strategy for exchanging manned metal for RPAs? What are the budget implications of this strategy in an increasingly austere fiscal environment? These are increasingly difficult questions requiring reflection by the Total Force.

## Conclusion

While a considerable ethical debate has swirled around the use of RPAs, US military employment has consistently demonstrated a position that RPAs require no more concern or governing than any other emerging technology.[45] Today, RPAs are viewed appropriately as merely an extension of a long historical trajectory of displacing warriors from their foes, for the warrior's better protection.[46] However, reflecting on in-theater and in-garrison risks to both combatants and non-combatants, it is clear in the RPA world, the doctrine of double effect increasingly cuts both ways.

In the near future, RPA operations may not exclusively be a virtual "away game." This is particularly true if a sovereign nation attacks the RPA infrastructure in the US. Just because

such an attack hasn't happened yet does not mean it is not a threat -- and such an attack could be legal, legitimate, and devastating. As the homeland becomes increasingly part of the battlespace, the military must recognize and address this reality now with specific solutions and risk-mitigating measures. Likewise, in the larger view, as the military continues its current strategic inclination toward more autonomous warfare, it is essential the just war implications of this trend be addressed in concert with new technology development. If it does not, the RPA community, the USAF, and the nation will likely suffer serious debilitating strategic and operational consequences.

## Notes

[1] Office of the Secretary of Defense. "Unmanned Systems Integrated Roadmap FY2011-2036." http://www.defenseinnovationmarketplace.mil/resources/UnmannedSystemsIntegratedRoadmapFY2011.pdf, 13.

[2] Headquarters, United States Air Force, *United States Air Force Unmanned Aircraft Systems Flight Plan 2009-2047*. (Washington DC: Department of the Air Force, 18 May 2009), 15, 27.

[3] House, *Civil Liberties and National Security: Hearing Before the Subcommittee on the Constitution, Civil Rights and Civil Liberties*, 111th Cong., 2nd sess., 9 December 2010, 57.

[4] *Air Force Operations and the Law*. (Maxwell AFB, AL: The Judge Advocate General's School, 2009), 248.

[5] Ibid., 249.

[6] Department of Defense, *Conduct of the Persian Gulf War, Final Report to Congress* (Washington, DC: Government Printing Office, 1992), 613.

[7] Article 43 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

[8] *Military Commissions Act of 2006*. Public Law 109–366, 109th Cong., (17 October 2006), 948a.

[9] House, *Civil Liberties and National Security: Hearing Before the Subcommittee on the Constitution, Civil Rights and Civil Liberties*, 55.

[10] *The Military Commander and the Law*. Maxwell AFB, AL: The Judge Advocate General's School, 2012. 668.

[11] International Committee of the Red Cross, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law Adopted by the Assembly of the International Committee of the Red Cross on 26 February 2009,* 993.

[12] Ibid., 993.

[13] Article 51 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1) (2nd part).

[14] International Committee of the Red Cross, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law Adopted by the Assembly of the International Committee of the Red Cross on 26 February 2009*, 996.

[15] "What are jus ad bellum and jus in bello?" http://www.icrc.org/eng/resources/documents/misc/ 5kzjjd.htm (accessed 2 December 2012).

[16] Michael Walzer, *Just and Unjust Wars*. (New York, NY: Basic Books, Inc., 1977), 135.

[17] *Air Force Operations and the Law*, 249.

[18] Alex J. Bellamy, *Just Wars*. (Cambridge, UK: Polity Press, 2006), 124.

[19] Ibid., 124.

[20] Michael Walzer, *Just and Unjust Wars*, 153.

[21] United Nations Charter, Article 51.

[22] Harold Koh, Legal Advisor to the US Dept of State. "The Obama Administration and International Law." Presentation. Washington DC: Annual Meeting of the American Society of International Law, 25 March 2010, 15.

[23] Ibid., 15.

[24] *The Military Commander and the Law*, 667-669.

[25] International Committee of the Red Cross, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law Adopted by the Assembly of the International Committee of the Red Cross on 26 February 2009*, 1001.

[26] Harold Koh, "The Obama Administration and International Law.", 15.

[27] International Committee of the Red Cross, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law Adopted by the Assembly of the International Committee of the Red Cross on 26 February 2009*, 1021.

[28] Ibid., 1032.

[29] Ibid., 1009.

[30] Ibid., 1021.

[31] Marco Sassòli, "Legitimate Targets of Attacks Under International Humanitarian Law." *Background Paper prepared for the Informal High-Level Expert Meeting on the Reaffirmation and Development of International Humanitarian Law, Cambridge*, 27-29 January 2003, 9.

[32] "No to U.S. Drone Strikes." A diagram in "Global Opinion of Obama Slips, International Policies Faulted." Pew Research Center. 13 June 2012. http://www.pewglobal.org/2012/06/13/global-opinion-of-obama-slips-international-policies-faulted/ (accessed 14 November 2012).

[33] Ibid.

[34] Rebecca Grant, "RPAs for All," *Air Force Magazine*, August 2012, 54.

[35] Office of the Secretary of Defense. "Unmanned Systems Integrated Roadmap FY2011-2036.", 1-2.

[36] *Air Force Operations and the Law*, 249.

[37] Ibid., 249.

[38] MACDILLAFBI31-100, *Security Education and Training*, 12 April 2010, 4.

[39] "What is NIMS?" http://www.fema.gov/frequently-asked-questions-2/ (accessed 6 December 2012).

[40] John Reed, *Air Force Chief Wary of Cyber 'Black Hole,'* http://killerapps.foreignpolicy.com/posts/2012/09/18/air_force_chief_wary_of_cyber_ black_hole (accessed 1 December 2012).

[41] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *Institute for Information Technology Applications*. June 1999, 6-8.

[42] Charles J. Dunlap Jr., "The Ethical Dimensions of National Security Law," *South Texas Law Review 2009*, 793.

[43] John A. Tirpak, "Thinking About Counterspace," *Air Force Magazine*, January 2013, 9.

[44] William Matthews, "Looking Ahead to 2020," *National Guard*, September 2012, 33.

[45] House, *Civil Liberties and National Security: Hearing Before the Subcommittee on the Constitution, Civil Rights and Civil Liberties*, 54.

[46] Bradley Jay Strawser, "Moral Predators: The Duty to Employ Uninhabited Aerial Vehicles," *Journal of Military Ethics*, Volume 9 No. 4, 2010, 343.

## Bibliography


AFDD 3-60 Change 1, *Targeting*, 28 July 2011.

*Air Force Operations and the Law*. Maxwell AFB, AL: The Judge Advocate General's School, 2009.

Article 43 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977

Article 51 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1), 8 June 1977.

Article 52 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

Becker, Thomas and Lt Col Richard L. Dashiell. (Academic Directors, The JAG School). Interview, 9 November 2012.

Bellamy, Alex J. *Just Wars*. Cambridge, UK: Polity Press, 2006.

Boot, Max. *War Made New: Technology, Warfare, and the Course of History, 1500 to Today.* New York, NY: Gotham Books, 2006.

Boothby, Bill. "And For Such Time As: The Time Dimension to Direct Participation in Hostilities." *International Law and Politics* [Vol. 42:741], 2010.

Coppieters, Bruno and Nick Fotion. *Moral Constraints on War*. New York, NY: Lexington Books, 2008.

Dains, Ron. "Societal Issues: CONUS-Based Remotely Piloted Aircraft Operations: Exploring the Implications of Expanding the Battlespace." Presented at the 2010 AETC Symposium, 14-15 Jan 2010.

Department of Defense. *Conduct of the Persian Gulf War, Final Report to Congress*. Washington DC: Government Printing Office, 1992.

Dunlap, Major General Charles J. "Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber Warriors." *Nebraska Law Review*, Vol. 87:712. (16 July 2008): 712-724.

Dunlap, Major General Charles J. "The Ethical Dimensions of National Security Law." *South Texas Law Review 2009*, 789-801.

"Global Opinion of Obama Slips, International Policies Faulted." *Pew Research Center*. 13 June 2012. http://www.pewglobal.org/2012/06/13/global-opinion-of-obama-slips-international-policies-faulted/ (accessed 14 November 2012).

Grant, Rebecca. "RPAs for All." *Air Force Magazine*. August 2012, 54-57.

Gruen, Major Patricia. "Targeted Killing: Legitimate Self-Defense or Illegal Warfare Tactic." Draft Elective Paper, ACSC, 2012.

Guiora, Amos. "Targeted Killing as Active Self Defense." *Case West Law*, 2005, citing Emanuel Gross, "Thwarting Terrorist Acts by Attacking the Perpetrators or Their Commanders as an Act of Self-defense: Human Rights versus the State's Duty to Protect its Citizens", *TEMPLE INT'L & COMP L. J.*, 2001.

Headquarters, United States Air Force. *United States Air Force Unmanned Aircraft Systems Flight Plan 2009-2047*. 18 May 2009.

Hensel, Howard M., Editor. *The Law of Armed Conflict. Constraints on the Comtemporary Use of Military Force*. Burlington, VT: Ashgate Publishing Company, 2007.

International Committee of the Red Cross. *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law Adopted by the Assembly of the International Committee of the Red Cross on 26 February 2009*.
Joint Publication (JP) 3-26, *Homeland Security*, 2 August 2005.
Jones, Lt Col Stephen R. (17 RS/CC). Interview, 30 September 2012.
Koh, Harold. Legal Advisor, US Department of State. "The Obama Administration and International Law." Annual Meeting of the American Society of International Law, Washington DC, 25 March 2010.
Kolff, D. W. "Missile Strike Carried Out with Yemeni Cooperation' – Using UCAVs to Kill Alleged Terrorists: A Professional Approach to the Normative Basis of Military Ethics." *Journal of Military Ethics*, 2(3) 2003: 240–244.
Libicki, Martin C. "The Specter of Non-Obvious Warfare." *Strategic Studies Quarterly*, Fall 2012, 88-101.
MACDILLAFBI31-100, *Security Education and Training*, 12 April 2010.
Matthews, William. "Looking Ahead to 2020." *National Guard*, September 2012, 33.
Mayer, Jane. "The Predator War: What are the risks of the CIA's covert drone program?" *The New Yorker*, October 2009. http://www.newyorker.com/reporting/2009/10/26/091026fa_ fact_mayer (accessed 26 October 2012).
*Military Commissions Act of 2006.* Public Law 109–366, 109th Cong., 17 October 2006.
Office of the Under Secretary of Defense. *2006 Unmanned Aircraft Systems Roadmap: 2005–2030.* Washington, DC: Office of the Under Secretary of Defense, 2006.
Office of the Secretary of Defense. *Unmanned Systems Integrated Roadmap FY2011-2036.* http://www.defenseinnovationmarketplace.mil/resources/UnmannedSystemsIntegratedRoadmapFY2011.pdf. (accessed 26 November 2012).
O'Neal, Brain (Las Vegas Fire Captain). Interview, 16 December 2012.
Phythian, M. *Ethics and Intelligence: The Implications of the Rise of the Armed Drone.* Paper presented at 7th Global Conference on War and Peace, Prague, 30 April 2010.
Pictet, Jean. "Commentary on Geneva Convention IV Relative to the Protection of Civilian Persons in Time of War (1958)." 1994 reprint edition, 51.
Pub. L. No. 109-366, 120 Stat. 2600 (Oct. 17, 2006), enacting Chapter 47A of title 10 of the United States Code (as well as amending section 2241 of title 28).
Reed, John. "Air Force chief wary of cyber 'black hole.'" http://killerapps.foreignpolicy.com/posts/2012/09/18/air_force_chief_wary_of_cyber_black_hole (accessed 1 December 2012).
Riza, Lt Col M. Shane. "KILLING WITHOUT HEART: Limits on Robotic Warfare in an Age of Persistent Conflict." Industrial College of the Armed Forces, 2010-2011.
Sassòli, Marco. "Legitimate Targets of Attacks Under International Humanitarian Law." *Background Paper prepared for the Informal High-Level Expert Meeting on the Reaffirmation and Development of International Humanitarian Law, Cambridge*, 27-29 January 2003.
Schmitt, Michael N. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *Institute for Information Technology Applications.* June 1999, 1-41.
Seffers, George I. "Era of Change for Unmanned Systems." *Signal*, November 2012, 34-37.
Singer, P.W. *Wired for War*. New York, NY: Penguin Books, 2009.

Steinhoff, U. “Jeff McMahan on the Moral Inequality of Combatants.” *Journal of Political Philosophy*, 2008 16(2): 220–226.
Strawser, Bradley Jay. *Moral Predators: The Duty to Employ Uninhabited Aerial Vehicles*. Journal of Military Ethics, Vol 9 No. 4, 2010, 342-468.
Sullivan, Gordon R. “Preface, U.S. Army Unmanned Aircraft Systems: Changing Modern Warfare.” *AUSA Torchbearer*, July 2010, 1-4.
Third Geneva Convention.
*The Military Commander and the Law*. Maxwell AFB, AL: The Judge Advocate General’s School, 2012.
Tirpak, John A. “Thinking About Counterspace.” *Air Force Magazine*. January 2013, 9.
United Nations Charter, Article 51.
US House of Representatives. *Civil Liberties and National Security: Hearing Before the Subcommittee on the Constitution, Civil Rights and Civil Liberties*. One Hundred Eleventh Congress, 2nd sess., 9 December 2010.
United States Joint Forces Command. *Joint Concept of Operations for Unmanned Aircraft Systems*. April 2010.
Walzer, Michael. *Just and Unjust Wars*. New York, NY: Basic Books, Inc., 1977.
Waxman, Matthew C. *International Law and the Politics of Air Operations*. Santa Monica, CA: Rand, 2000.
‘What are jus ad bellum and jus in bello?” http://www.icrc.org/eng/resources/documents/misc/5kzjjd.htm (accessed 2 December 2012).
“What is NIMS?” http://www.fema.gov/frequently-asked-questions-2 (accessed 6 December 2012).